RADIO TV REPORTS, INC.

4701 WILLARD AVENUE, CHEVY CHASE, MARYLAND 20015 656-4068

FOR PUBLIC AFFAIRS STAFF

PROGRAM The MacNeil-Lehrer Report STATION WETA-TV
PBS Network

DATE April 21, 1982 7:30 pm CITY Washington, D.C.

SUBJECT Cryptography

ROBERT MACNEIL: In recent months, the Reagan Administration has been trying to clamp down on the flow of sensitive information to the Soviet Union. The Administration sees what it calls a hemorrhage of scientific and technological secrets to the Soviets and other unfriendly countries. The efforts to stop it have caused anxiety in the academic community, particularly the veiled threat of government censorship of scientific information.

Twice in recent months, Admiral Bobby Inman, Deputy Director of the CIA, has told scientists that if they didn't practice voluntary restraint in publishing scientific information, the government might impose it. Many scientists say such restraint would violate their academic freedom and stifle research. They talk of the risks of importing Soviet-style secrecy into American life.

Tonight, how can this country protect national security and yet maintain an open society?

JIM LEHRER: Robin, surprisingly, the area where the conflict has been most severe and most lengthy has been cryptography, the science of codes, making them and breaking them. For centuries, it had been the exclusive, secretly exclusive domain of soldiers and spies. There was no need for civilians to be tinkering around with cryptography. So few did. But along came the computer. Business and industry store much information on computers, information they want to keep private, most particularly from competitors. So suddenly there was a civilian need for cryptography, from computer codes that couldn't be broken. Cryptology researchers in the private domain went to work. Soon the new advances worried the government, particularly the National

Security Agency, the super-secret intelligence agency which does the coding and decoding for the United States Government.

In the late '70s, Bobby Inman was head of NSA, and he declared the unrestrained public discussion of cryptographic research threatened our national security, by making it easier for the Soviets and others to develop better codes and to break ours. The private cryptography community and the government have been sparring over the issue ever since.

MACNEIL: The cryptography issue actually surfaced four years ago, when a computer scientist applied for a patent for a coding device he'd invented. The National Security Agency slapped a secrecy order on his invention, but he fought it and he won.

That led to the formation of a panel to consider the national security aspects in cryptography work. The panel recommended that scientists submit their research to the NSA before publication.

The scientist whose work started the fuss is George DeVita of the University of Wisconsin at Milwaukee.

Why did you fight the agency's order to keep your invention secret?

GEORGE DEVITA: Well, Robin, basically I fought it because I thought it was unecessary to clamp any kind of secrecy on work that's fundamentally a mathematical subject. Its principles are very difficult to really control and to hide. Basically, the encryption algorithms that we tend to devise in the academic community are based on relatively simple mathematical principles and electrical engineering principles. So I found it difficult to see how such principles could in fact be kept under wraps.

But more importantly, I felt that encryption was indispensable to the protection of data, particularly as the society gets more computerized. It has become practically impossible to keep plugging up loopholes in computer systems that keep cropping up every now and then. And I feel that encryption really is the only effective method that we can use to protect that data.

MACNEIL: Things like your bank record or health records or things like that, which are kept on computers, could be -- could be stolen or looked at by people we didn't want to unless they were encoded. Is that it?

DEVITA: Yes. The computerization of society, Robin, has proceeded at an extremely rapid rate. We have thousands of data bases concerning medical records, credit records, our purchasing habits, electronic mail that is coming in rather shortly. All of these data bases and communication networks that are being established are basically vulnerable to all kinds of attacks. And the only really effective method that we can use to protect data while it is being stored on disks or while it's traveling on the electronic wires is to encrypt these messages or this data.

MACNEIL: How do you know that your particular device was not -- would not have damaged national security if, say, the Soviets had obtained it?

DEVITA: Well, basically, I find the argument that research will lead to any kind of damage or harm to the mission of NSA, and hence national security in general, I find it very difficult to really believe. Because encryption is a very difficult subject matter to control. We're not the only ones who do research on encryption, first of all.

Second, the kind of principles that we engage in are not likely to lead to any kind of accidental discovery of codes that NSA uses, because we don't really know what NSA uses, nor do we want to, for example, know what NSA uses.

And as for the codes leading to any kinds of denial of intelligence gathering to NSA, I'd say the probabiligy of that is rather low. Because, in principle, most of the systems are not unbreakable. In fact, they're breakable. So I find the arguments that we have suddenly devised techniques that would deny NSA the intelligence-gathering capability, I find them very difficult to believe. In fact, historically, every important code has been broken.

MACNEIL: Now, you were a member of this panel set up after the incident with your device, which then recommended -- and it's been the practice ever since -- that people in your field would submit scientific papers and findings to the NSA before they publish them, and they do it voluntarily. But you, alone on that panel, disagreed and opposed that. Why did you disagree?

DEVITA: For many reasons. Again, one of the reasons is that I felt that encryption is an extremely important technology for civilian applications. But other reasons were reasons of fears that that decision would lead to more formal restraints on academic freedom that I didn't think should be instituted, slowly, voluntarily initially, and subsequently, perhaps, with legislation. I felt the decision was a rather unwise one at the time.

MACNEIL: Now, that's been working for a year. And scientists, unlike you, have been submitting their papers to the NSA. Has any harm come of that?

DEVITA: Well, it's not clear to me how it has worked or not worked, because -- again, I don't know what NSA in fact does get or does not get. I believe that the issues of sending materials to NSA are not really the real issues here. I believe that many people would send things to NSA voluntarily, but I don't believe that really calls for any kind of system to be instituted for formal prior review at all. I think NSA can easily ask most authors to send them their papers, and they probably would. I do.

MACNEIL: You do it anyway.

DEVITA: I would do it anyway. I don't find any reason for any kind of formal mechanism to have NSA request our papers. They can simply get on our mailing list and they can get the papers ahead of time.

MACNEIL: Is it possible, is it practicable for the government to restrict the dissemination of this kind of information in the cryptology field, these devices? You have two of them in front of you here.

DEVITA: No, not at all. And that's one of the key arguments that I try to make in this whole debate about protecting this kind of technology.

Here we have an encryption device which is actually the government-approved data encryption standard. This particular board happens to be an encryption and decryption device. This is, of course, controlled. You cannot export this without a license from the Commerce Department.

On the other hand, here we have a general purpose computer which can be also made into an encryption device rather easily. All you would need is a program.

So, effectively, these two board are almost identical.

MACNEIL: And one is restricted and the other isn't.

DEVITA: That's correct. And the argument is that we cannot control this technology because microprocessors, which is really this chip at the top of the board, are abundant and inexpensive. And furthermore, we're not the only ones who make these microprocessors. The Japanese and the Germans and the British, everybody else is making these microprocessors. So it would be very difficult to really control the materials that go into making crypto systems.

MACNEIL: Well, thank you.

LEHRER: Also on that panel which devised the voluntary review plan was Daniel Schwartz. Mr. Schwartz was then the general counsel for the National Security Agency. Since last October, he's been in the private practice of law here in Washington.

Mr. Schwartz, has the voluntary system worked, in your opinion?

DANIEL SCHWARTZ: It has so far. It has basically been in effect, in a formal sense, for about six months. But there has been quite a long period of time in which researchers in this field have been submitting papers.

LEHRER: How many papers have been submitted, in rough terms?

SCHWARTZ: Since the initiation of the program, some 35 papers have been submitted. But there were papers submitted before that. The problem was that they were not routinely submitted by everyone doing writing in the field.

LEHRER: Well, of these 35, were any of them killed by the NSA?

SCHWARTZ: None of -- all of the papers have gone forward through their publishing process, at least have not been restrained by NSA in any way. A few of the papers have raised some problems, and an accord has been reached with the authors in each case for minor changes in the papers.

LEHRER: But without exception, all 35 did go ahead. They were published. Is that right?

SCHWARTZ: They haven't actually been published...

LEHRER: I know what you mean. They went through the process and they were cleared.

All right. If there hasn't been any need to kill any papers or to prohibit the publication of any of the papers, doesn't that prove that the concern over the cryptography and the publication of these papers was not founded on fact?

SCHWARTZ: No, for two reasons. First of all, a six-month period is a very short period, particularly in a science like this. The study group recommended that the results of this voluntary process be reviewed after two years to see what kind of results had occurred and how NSA had dealt with the academic community. I would say six months is simply too short to make that judgment.

Secondly, there have been some changes that have been made where there was some feeling, in fact, that it would be disadvantageous to the national security to have the papers go as submitted.

LEHRER: I mean were these serious problems? And I realize you can't tell me what they were. I wouldn't probably understand it if you did. But I mean were they serious problems, that if those papers had not been changed, that there would have been serious harm to the national security? Or were they little things?

SCHWARTZ: I don't know how you make that kind of a judgment. You can't really make that kind of a judgment until you see what the results are. Very often, particularly, in the field of cryptology, it is impossible to trace the result. You really don't know who's reading what, and you really don't know what kind of effect it has.

Part of the problem in this whole field is one that Dr. DeVita mentioned. As he said, he doesn't know what NSA does He doesn't know what the U.S. Government does. The problem is that most scientists in this area have no real idea whether what they're writing on might have an impact on the national security.

Part of the interest in establishing this kind of program was to give scientists an opportunity, and on a voluntary basis, to determine whether, in fact, there might be some impact in what they were writing. They wouldn't independently know that.

LEHRER: What about Mr. DeVita's point that it's really impossible to control the flow of this kind of information on crytography. It's a very -- you know, his example of the two boards there, that they're identical, you just have to make a minor change. And one board is available anywhere; the other one is restricted.

SCHWARTZ: There is no intent, I think, here, realistically, to get a perfect system. What one would be seeking, at best, is some incremental advantage, some additional help in trying to limit the outpouring of technical data that might be of assistance to our actual or potential adversaries. It's very hard to stem it completely, as we know. But the hope would be that in various -- in various ways, that this could be limited.

LEHRER: When Admiral Inman made his statement -- I think it was in 1979 -- saying that the free discussion, or the open discussion of cryptography was endangering the national security, did he have a specific incident in mind, that something had happened to prove his point? Or was it a fear based on what he was seeing that might happen?

SCHWARTZ: Two things were happening during that period. One was, there was an increased amount of research, and therefore publication, in the field of cryptography. This is an inevitable development. The concern was that that would raise problems, potentially. And there were incidents where, in fact, it did raise fairly serious concerns.

The second thing that happened, however, was that there have been -- in part because the National Security Agency was such a secret and highly classified agency -- a real lack of a dialogue between that agency and the scientific community. And part of what Admiral Inman was calling for at that time, and part of what this study group provided, was a vehicle to have a dialogue to address the problem.

LEHRER: And you think that's on its way, that's in progress.

SCHWARTZ: Well, so far, it is on its way. There has been, as far as one can tell, a fairly good response. And we will just have to see in the long term.

LEHRER: Thank you.

MACNEIL: Now a view from the Reagan Administration. Stephen Bryen is Deputy Assistant Secretary for International Economic Trade and Security Policy at the Defense Department.

Mr. Secretary, Admiral Inman warned that if some voluntary restraint did not happen, government -- and he mentioned the Pentagon specifically -- might be forced to step in. Do you agree with that?

SECRETARY STEPHEN BRYEN: Well, I think what we might have to do, if we can't work a system of voluntary restraint, is consider how we manage our own in-house research and development, and particularly the contract research that goes out to universities and scientific organizations around the country.

MACNEIL: You mean if they didn't voluntarily restrict publication of information, you would bring that research inside the Pentagon, so to speak.

SECRETARY BRYEN: It's a possibility, but I think a slight possibility, because, in fact, I expect we will have very good cooperation from our scientific community. We are engaged now in the beginning, only the beginning, of a dialogue on this subject. I think we can become more precise about the things we desire. And I believe that the scientific community is going to be very responsive.

MACNEIL: Are you doing some planning in the Defense Department right now for some ways of the government restricting this dissemination of the scientific community does not cooperate?

SECRETARY BRYEN: Only in a very limited sense. We are beginning to try and specify what particular programs we should be extremely careful about, in terms of how we deal on the outside. I think in the past...

MACNEIL: Do you mean we, Pentagon, or we, American?

SECRETARY BRYEN: We, Pentagon.

There are some sensitive programs that we have that were fairly loosely managed in the past, and we're trying to tighten those up a bit. I doubt that anyone on the outside would even see where the tightening occurs, but we will know.

MACNEIL: Do you care to mention an example?

SECRETARY BRYEN: One of the programs that we are quite concerned about is the very-high-speed integrated ciruit program we have underway in the Pentagon. We don't mean to tighten it up to the point where it becomes an entirely in-house effort, because I think we would fail at that. But we do mean to be very careful about the very specific circuits that apply to military hardware.

MACNEIL: I see.

Now to the point of what the need is for all this restriction. I read a figure today, and I've forgotten what the source of it was, but an estimate that only one percent of the so-called hemorrhage of sensitive information to, say, the Soviet Union could be traceable to the scientific community and publication, and that most of it comes from other sources, spying and so on.

SECRETARY BRYEN: The answer is we don't know the answer. We have tried, ourselves, to come to grips with how much is transferred through open literature, how much through trade conference, how much through legal sales -- and quite a lot was in the past transferred through legal sales -- how much through illegal acquisition. And we simply don't know today what the proportions are.

What we do know is that everywhere we look we find a plethora of examples of transfers of very sensitive technology that have gone to the Soviet bloc, have been turned around and used in Soviet military hardware. That much we do know.

I must say it's a very difficult area to be precise in, but we are trying to find more of the answer. Because, obviously, how we use our own resources will depend on the outcome.

MACNEIL: Can some parts of science be placed off limits, on national security grounds, when they have become vital in civilian life? Take the example of cryptography, as we've just heard from Professor DeVita.

SECRETARY BRYEN: I don't think so. I think some very special areas that relate directly to military applications can be assigned a special status and category. But I should mention for the record that in many cases today civilian technology is actually well in advance of the kind of technology that's embodied in the weapons systems that defend this nation. That's one of the great problems that we face today. It's something that the Soviets are well aware of and are exploiting.

MACNEIL: You mean that, unwittingly, a scientist like Professor DeVita could invent something that was way ahead of anything you were actually using or planning to use.

SECRETARY BRYEN: Absolutely.

MACNEIL: And not know it.

SECRETARY BRYEN: Possibly not know it.

MACNEIL: I see. Well, thank you.

LEHRER: A second and different overview now from William Carey, Executive Director of the American Association for the Advancement of Science, the largest general science group in the country, one vitally involved in this issue of scientific information an national security.

Mr. Carey, how is the scientific community reacting to the Inman call for voluntary restraint?

WILLIAM CAREY: I think with consternation and disbelief. The shock that was administered to science by Admiral Inman's remarks was considerable.

It is not that science, in any way, is against the national security. That is not the problem. Science has supported the national security in the last 35 years through three hot wars and one very long cold war, and it will continue to do so. The issue arises over the imposition of censorship, whether compulsory or voluntary.

LEHRER: There is a difference, though, isn't there, between -- or do you not see a difference between voluntary censorship and compulsory censorship?

CAREY: Of course there is a difference. In the one case, the voluntary censorship, science cooperates with the national security authorities. In the other case, science has no choice.

LEHRER: Well, let's take the voluntary first. What is the basic objection to voluntarily going along with Bryen and Schwartz? Schwartz is a former employee, I should say.

CAREY: The objection is the generality in which the government side has presented or stated what the problem is. When Admiral Inman, who is a superb public servant, by the way, spelled out a long laundry list of areas of technology and applied science and general science to make his point, he did not discriminate among fields of science or among the technological intensities of technology versus research. And it makes a very big difference.

He has now proceed to think it over a little more. And what he is now telling the Congress is that 70 percent or more of the so-called hemorrhage -- which I believe is now referred to as leakage -- comes from high technology which is embedded, in many ways, in American manufacturing, goods or products, or in process technology.

Now, I don't think that very many people in the scientific community would argue with that proposition. But the remaining 30 percent of the problem comes down applied research, mainly in the industrial area, where the information seems to leak out through business deals, through legal and illegal arrangements.

And then you get down to science, the discovery process, the searching process, the creative process. And it may very well be that we're talking about one or two percent of the problem that the national security people are concerned about, one or two percent on a scale of 100 percent, defining the entire problem. And when government shakes a finger at scientists and says, "If you don't submit to a voluntary system of bringing to government information, your ideas, what are you going to do research on, if you don't send us copies of your publication or your preprints before you allow them to go into the system, then there'll be a public outcry and Congress will get after you and make it worse," well, the difficulty is that the way science works is -- it's like billiards. Your idea caroms off my thinking and off the thinking of a third scientist and a fourth. And in each collision, and in the total collision, the idea matures. It's changed. It's altered. And this is the way discovery works, the way knowledge advances. And finally, out of this collision, there comes an idea, a new idea, a new piece of information that fits into the jigsaw of knowledge.

And that's what would be impaired if the arteries of communication were clamped off for very serious reasons, coming from the government side. You clamp those arteries off, you're going to shut off the blood, you're going to slow down science, and you're going to invite second-rate science, which will not keep our national defense ahead of the Soviets. That's the problem.

LEHRER: Thank you.

MACNEIL: Mr. Secretary, what's your answer to that?

SECRETARY BRYEN: Well, I think our answer is as follows: We agree entirely that a completely broad-brush government approach is not necessary, is not called for, is not desirable. I agree fully to the notion that we want to keep our scientists as unfettered as we possibly can.

I think we have a responsibility, therefore, to try and be precise about the areas where we have concern, as happened in the area of cryptology, as will, I hope, happen in the area of very-high-speed integrated circuits, and other areas that are identified in precise terms.

What we need to then have is a dialogue with our university people and with our research organizations so that we can work out reasonable solutions with the least amount of, even voluntary, restrictions.

MACNEIL: What's wrong with that, Mr. DeVita?

DEVITA: Well, I think it's very difficult, really, to assess the damage that's done to a scientific effort when you withhold even a small number results. I think that the voluntary system really envisions withholding some results when NSA objects to them.

MACNEIL: Is that what it does envision, Mr. Secretary?

SECRETARY BRYEN: Well, I don't know if it does. I think that there are certain results that we would rather not publish that could bring harm to this country. We have a pretty good idea what they are by now. I think our scientific community that works on these problems has a pretty good idea of what they are.

MACNEIL: Well, Mr. Schwartz, you've thought about this a lot. What do you say -- I think Mr. DeVita and Mr. Carey have made the same point, that, in his image, the billiard game would be slowed down. You wouldn't have the number of collisions that produce new ideas if you stop publishing even a few.

SCHWARTZ: First of all, in practice, what happens, at least in the field of cryptology, is that there is a review. And so far, there has been very little effect on the final published work.

Secondly, I think it's important to stand back and look at what's really asked for here. What was done in the field of cryptology, and I think what Admiral Inman asked for, was a dialogue, recognizing that there are very important concerns on both sides. In the cryptology, with that study group, in fact, the original proposals that Admiral Inman had suggested were completely rejected. But the people on the study group -- and I was the only government representative. The people on the study group came up with an entirely different proposal that is now being tried.

MACNEIL: Can I just interrupt? We just have a few seconds. I wanted to get Mr. Carey's view.

Mr. Carey, is the scientific community going to cooperate the way Secretary Bryen hopes it will?

CAREY: The scientific community is going to do its best to find an accommodation, to find a balance. I think that's going to be a very difficult, very responsible process. The National Academy of Sciences is working on that. We are setting up a panel. It has begun to meet.

MACNEIL: But you think it's going to be very difficult.

CAREY: It's going to be difficult, but I think we will make some ground, we will gain some ground, and come into some kind of understanding. We have to.

MACNEIL: And we have to leave it there.